Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of allocating an address to a certificate to ~~be stored~~ enable the storage of said certificate in an addressable database for subsequent retrieval and use in a cryptographic system, said method comprising the steps of:_____

    ___generating a string for use as a certificate locator, said string being generated from information contained in a ~~certificate~~ request for said certificate; and_____

    ___utilizing said string to obtain said address for retrieving a corresponding certificate from said database.

2. (currently amended) A method according to claim 1 wherein said string is mapped to an address in said ~~directory~~ database.

3. (currently amended) A method according to claim 1 wherein said string is used as said address in said ~~directory~~ database.

4. (original) A method according to claim 1 wherein a mathematical function is applied to said information to obtain said string.

5. (original) A method according to claim 4 wherein said mathematical function is a hash function.

6. (original) A method according to claim 5 wherein said string is a portion of the output of said hash function.

7. (currently amended) A method of identifying to a recipient, an address of a certificate ~~to a recipient~~ of a signed message in a data communication system, said method comprising the steps of preparing a set of information for inclusion in a certificate request, generating from said set of information a string for use as a certificate locator to enable a corresponding certificate to be located in a database, and forwarding said string to said recipient to indicate

5

the location of said certificate in said database <u>for subsequent retrieval</u>.

8. (original) A method according to claim 7 wherein said information includes a time varying element.

9. (original) A method according to claim 7 wherein a predetermined mathematical function is applied to said information to obtain said string.

10. (currently amended) A method for maintaining certificates in a public key infrastructure having a certification authority and a pair of correspondents, said method comprising the steps of ~~collating~~ <u>collecting</u> at one of said correspondents<u>,</u> information comprising a request for a certificate of said certification authority, forwarding said request to said certification authority, computing <u>a string</u> from said information comprising said request ~~a string~~ for use as a certificate locator by said one correspondent and said certification authority, storing a certificate issued from said request in a ~~directory~~ <u>database</u> at an address ~~obtained~~ <u>being</u> <u>identifiable</u> from said string<u>,</u> and forwarding said locator from said one correspondent to another <u>of said correspondents</u> to permit retrieval of said certificate from said ~~directory~~ <u>database</u>.

11. (original) A method according to claim 10 wherein said information includes a time varying element.

12. (original) A method according to claim 10 wherein communication between said one correspondent and said certification authority is performed over a secure channel.

13. (currently amended) A method according to claim 10 wherein said other correspondent obtains an address of said certificate from a known address of said ~~directory~~ <u>database</u> and said string.

14. (original) A method according to claim 10 wherein said other correspondent forwards said locator to said certification authority for construction of said address.

15. (original) A method according to claim 10 wherein said string is computed by application of a cryptographic hash function at least part of said request.

16. (original) A method according to claim 15 wherein said part includes a time varying element.

17. (currently amended) A method according to claim 15 wherein a portion of the output of said hash function is used as said [[bit]] string.

18. (currently amended) A method according to claim 10 wherein said [[but]] string is utilised as a pointer to an address in a directory said database.